తెలుసుకొందాం



సైబర్ ఆర్థిక నేరగాళ్ళ మోసాల తీరు





రిజర్వ్ బ్యాంక్, ముంబై-2 (అంబుడ్స్‌మన్) వారు ముద్రించిన"Be(A)ware" అనే పుస్తకానికి
తెలంగాణ రాష్ట్ర సహకార అపెక్స్ బ్యాంక్, సహకార శిక్షణా సంస్థ (CTI) , హైదరాబాద్ వారి
తెలుగు అనువాదం.

ముందుమాట

గత కొన్ని సంవత్సరాలుగా మన దేశంలో డిజిటల్ (ఆన్‌లైన్) చెల్లింపులు గణనీయంగా పెరిగాయి. దీనివల్ల డబ్బు పంపించే విధానంలో సౌలభ్యం యేర్పడి వినియోగదారులకు యెంతో వెసులుబాటు కలగడమే గాకుండా భారత ప్రభుత్వం వారు తలపెట్టిన "ఫైనాన్షియల్ ఇంక్లూజన్" అంటే "అందరిని బ్యాంకింగ్ వ్యవస్థతో కలపాలనే సత్సంకల్పం" నెరవేరటానికి కూడా దోహదకారి అయ్యింది. ఎప్పుడైతే ఆన్‌లైన్ లావాదేవీలు పెరిగాయో, వాటితోపాటు ఆర్థిక (సైబర్) నేరాలు కూడా పెరిగాయి. ఆర్థిక నేరగాళ్ళు కొత్త కొత్త మాయోపాయాలతో సాంకేతిక పరిజ్ఞానం అంతగా లేనివాళ్ళనీ, ఆన్‌లైన్ లావాదేవీలకు కొత్తగా పరిచయమైనవాళ్ళనీ మోసగిస్తూ అమాయకుల కష్టార్జితాన్ని దోచుకొంటున్నారు.

ఈ పుస్తకం యొక్క ముఖ్యోద్దేశ్యం – "నేరస్థులు అలాంటి నేరాలు యెలా చేస్తారు? మనం తీసుకోవలసిన జాగ్రత్తల" గురించి సాధ్యమైనన్ని వివరాలను అందించటమే. ఇందులో పొందుపరిచిన వివారాలు కర్ణాకర్ణిగా విని వ్రాసినవి కావు. రిజర్వ్ బ్యాంక్ వారి అంబుడ్స్‌మన్ కార్యాలయాలకి అందిన అనేక ఫిర్యాదులని ఆధారం చేసుకొని పొందికగా వ్రాయబడ్డవి. సైబర్ ఆర్థిక నేరాలు చేసే విధానాలు (Modus operandi), వాటినుంచి మనం తీసుకోవలసిన జాగ్రత్తల (Precautions) గురించి సామాన్య ప్రజల్లో సదవగాహన కల్పించడానికి చేసిన చిన్న ప్రయత్నమే యీ పుస్తకం. బ్యాంకింగ్ పరమైన తమ తమ వ్యక్తిగత వివరాలు [ఎకౌంట్ నంబరు, యూజర్ ఐ,డి., పాస్ వర్డ్, సి.వి.వి (CVV)., ఒ.టి.పి, (OTP) వగైరాలు] తమవద్దే జాగ్రత్తగా వుంచుకోవటం, ఎవరికీ **తెలియజేయకపోవడం**, అంతే కాకుండా గుర్తు తెలియని వ్యక్తులనుంచి వచ్చిన టెలిఫోన్ కాల్స్ కి, ఈ-మెయిల్స్ కి స్పందించి వారికి మన వివరాలని **తెలియజేయకపోవడం** యెంత ముఖ్యమో యీ పుస్తకంలో మరీ మరీ చెప్పడమైనది. ఆన్‌లైన్ ట్రాన్సాక్షన్లలో మనం విధిగా పాటించవలసిన కొన్ని నియమాలు – ఉదాహరణకి 'పాస్ వర్డ్స్ తరచుగా మార్చుకోవడం', 'వ్యక్తిగత వివరాల గోప్యత' లాంటి వాటి గురించి కూడా సవివరంగా యీ పుస్తకంలో పొందుపరచడమైనది. ఈ పుస్తకం చదివి ఆ వివరాలను "తెలుసుకొందాం – జాగ్రత్తగా మసలుకొందాం".

రిజర్వ్ బ్యాంక్ వారు ఆంగ్లంలో ముద్రించిన [Be(A)ware] అనే పుస్తకాన్ని గ్రామీణ ప్రజల కోసం యథాతథంగా తెలుగులోకి అనువదించి మీకందిస్తున్న వారు – **"తెలంగాణ రాష్ట్ర సహకార అపెక్స్ బ్యాంక్ లిమిటెడ్, సహకార శిక్షణా సంస్థ, హైదరాబాద్"** వారి ఎకడమిక్ కన్సల్టెన్సీ విభాగం. ఈ పుస్తకం యెంతో మందికి సహాయ పడగలదని ఆశిస్తున్నాం.

తెలంగాణ రాష్ట్ర సహకార అపెక్స్ బ్యాంక్ లి. (TSCAB)
సహకార శిక్షణా సంస్థ (CTI) ఎకడమిక్ కన్సల్టెన్సీ విభాగం,
రాజేంద్రనగర్, హైదరాబాద్ 500030
సెప్టెంబర్ 2021.

Originally published in English by Reserve Bank of India, (Ombudsman), Mumbai-2 (Maharashtra & Goa)

Translated into Telugu by : S Satyanarayana, Academic Consultancy Wing, TSCAB, CTI , Hyderabad

Office of RBI Ombudsman, Mumbai-II
https://cms.rbi.org.in/



ఆర్థిక నేరగాళ్ళు నేరాలు చేసే విధానం – మనం తీసుకోవలసిన జాగ్రత్తలు

PART –A

బ్యాంకులు

"తెలుసుకొందాం – జాగ్రత్తగా మసలుకొందాం"
[Be(A)ware]



1. ఫిషింగ్ లింకులు (Phishing links)

నేరాలు చేసే విధానం

- బ్యాంక్‌లవో లేక యితర వ్యాపార సంస్థలవో అసలైన వెబ్‌సైట్ లా కనిపించేట్లు ఓ నకిలీ వెబ్ సైట్‌ను సృష్టించి, వాటిని వుపయోగించుకొని, అమాయకుల వ్యక్తిగత వివరాలు, పాస్ వర్డ్స్, యూజర్ ఐ.డి.లను కాజేయడాన్ని "ఫిషింగ్" అంటారు.
- బ్యాంక్‌లవో లేక యితర వ్యాపార సంస్థలవో అసలైన వెబ్‌సైట్ లా కనిపించేట్లు, నేరగాళ్ళు ఓ నకిలీ వెబ్ సైట్‌ను సృష్టిస్తారు.
- నేరగాళ్ళు యీ వెబ్‌సైట్ల లింకులను SMS ల ద్వారానో, సామాజిక మాధ్యమాల ద్వారానో, అంటే వాట్సాప్, ఫేస్‌బుక్, వగైరాల ద్వారానో, సామాన్య జనానీకానికి పంపుతారు.
- సాధారణంగా అలాంటి వెబ్‌సైట్లకు వెళ్ళేటప్పుడు అది 'అసలుదా ? నకిలీదా ?' అని ఎవరూ చూడరు. గోప్యంగా వుంచవలసిన తమ సమాచారాన్ని ఆ వెబ్‌సైట్ URL (Uniform Resource locator) వివరాలని పరీక్షించకుండా, అమాయకంగా ఆ నకిలీ వెబ్ సైట్ల లోని నేరగాళ్ళకి అందిస్తారు.
- నిజమైన / అసలైన వెబ్‌సైట్ల లా కనిపించే యీ దొంగ వెబ్‌సైట్లు మోసపూరితమైనవి. వీటిని పొరపాటున బ్రౌజ్ చేస్తే నేరగాళ్ళ చేతుల్లోకి వెళ్ళినట్లే.
- మనం తెలియక యీ వెబ్‌సైట్లలోకి వెళ్ళి, మన వివరాలు అందులో టైప్ చేసామో – అవన్నీ మోసగాళ్ళకి అందజేసిన వాళ్ళమవుతాం. జాగ్రత్త !!



మనం తీసుకోవలసిన జాగ్రత్తలు

మనకి తెలియని లింక్ లలోకి వెళ్ళకండి. SMS మెస్సేజీలు గాని, ఇ-మెయిల్స్ గాని, అపరిచిత వ్యక్తులనుంచి వచ్చినా, అనుమానాస్పదంగా వున్నా, ముఖ్యంగా మన బ్యాంక్ వివరాలు అడిగేవి వుంటే, వాటిని వెంటనే డిలిట్ చేయండి.



2. విషింగ్ కాల్స్ (Vishing calls)

నేరాలు చేసే విధానం

- ‘విషింగ్ కాల్స్’ అంటే మోసగాళ్ళు తమకు తాము ఏదో బ్యాంకర్ గానో, ఓ పేరుమోసిన కంపెనీ అధికారిగానో, ఏదో ఇన్సూరన్స్ ఏజంట్‌గానో, ప్రభుత్వోద్యోగి గానో, SMS మెసేజీలద్వారానో, సామాజిక మాధ్యమాల (వాట్సాప్, ఫేస్‌బుక్, ఇంటెర్నెట్, వగైరాల) ద్వారానో పరిచయం చేసుకొని, మన పేరో, ఫోన్ నంబరో, పుట్టిన రోజో (ముందుగానే తెలుసుకొని) మనకి చెప్పి నమ్మకాన్ని కలిగించి, గోప్యంగా వుండవలసిన మన వివరాలన్ని మననుంచి రాబట్టుకొంటారు.
- కొన్ని సార్లు, “అర్జంట్‌గా మీ వివరాలు చెప్పండి, లేకపోతే మీ ఎకౌంట్ బ్లాక్ చేస్తాం” అనో లేకపోతే “వెంటనే పెనాల్టి కట్టాలి లేకపోతే మీ ఎకౌంట్‌ని బ్లాక్ చేస్తాం” అనో లేకపోతే “క్రెడిట్ కార్డ్ మీద మీరు కట్టవలసిన వడ్డీ తగ్గిస్తాం” అనో మాయ మాటలు చెప్పి, వత్తిడి తెచ్చి, ఆలోచించుకొనేసమయం కూడా యివ్వకుండా మన బ్యాంక్ అకౌంట్ కి సంబంధించిన వివరాలన్ని అంటే ..యూజర్ ఐ.డి., పాస్‌వర్డ్, పిన్ కోడ్, CVV నంబరు.. యిలాంటివి సేకరించి మన ఎకౌంట్లో డబ్బుని కాజేస్తారు.

జాగ్రత్త !!



గుర్తుంచుకోండి

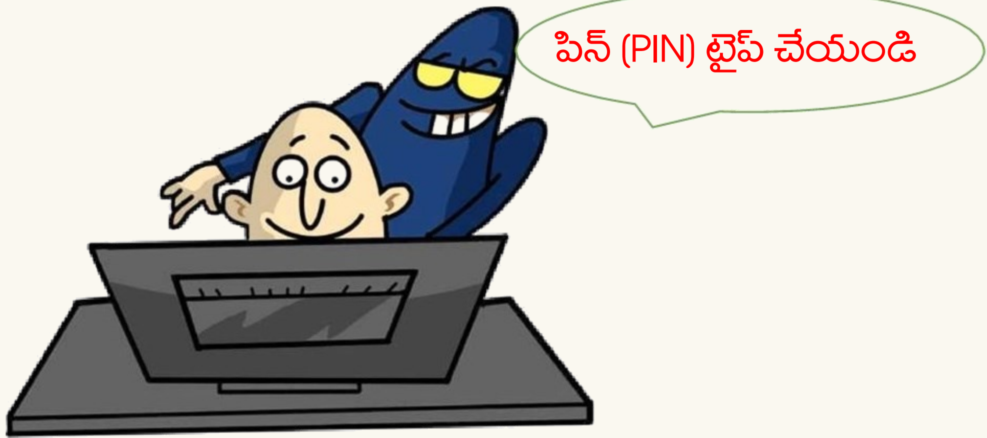
బ్యాంక్ అధికారులు, ఆర్థిక సంస్థలు, మరి ఏ యితర నికార్సైన వ్యాపార సంస్థలు – మీ యూజర్ ఐ.డి. గాని, మీ పాస్‌వర్డ్ గాని, మీ కార్డ్ వివరాలుగాని, CVV (Card verification value) గాని, వన్ టైమ్ పాస్ వర్డ్ (OTP) గాని యెట్టి పరిస్థితుల్లో **అడగరు.**



3. ఆన్ లైన్ లో జరిగే అవకాశాలున్న మోసాలు

నేరాలు చేసే విధానం

- ఒకవేళ మీరు వ్యాపారస్థులో, ఉత్పత్తిదారులో అయితే, మీరు తయారు చేసిన వస్తువులను 'ఆన్ లైన్ ద్వారా అమ్మిపెడతాం' అని నమ్మబలికిస్తారు.
- ఒక్కోసారి యేదో ప్రభుత్వ పథకం పేరుచెప్పి, తమకి తాము ప్రభుత్వోద్యోగులమని పరిచయం చేసుకొని, మీకు ఆ ఫలానా పథకం క్రింద 'డబ్బు పంపిస్తాం' అని నమ్మించి, మీకు డబ్బులు పంపకుండా, 'డబ్బులు పంపించండి (Request for money)' అనే ఆప్షన్ ద్వారా, మీ చేత ఆ రిక్వెస్ట్ ని ఒప్పింపచేసి, మీ ఎకౌంట్లోని డబ్బుల్ని లాగేసుకొంటారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

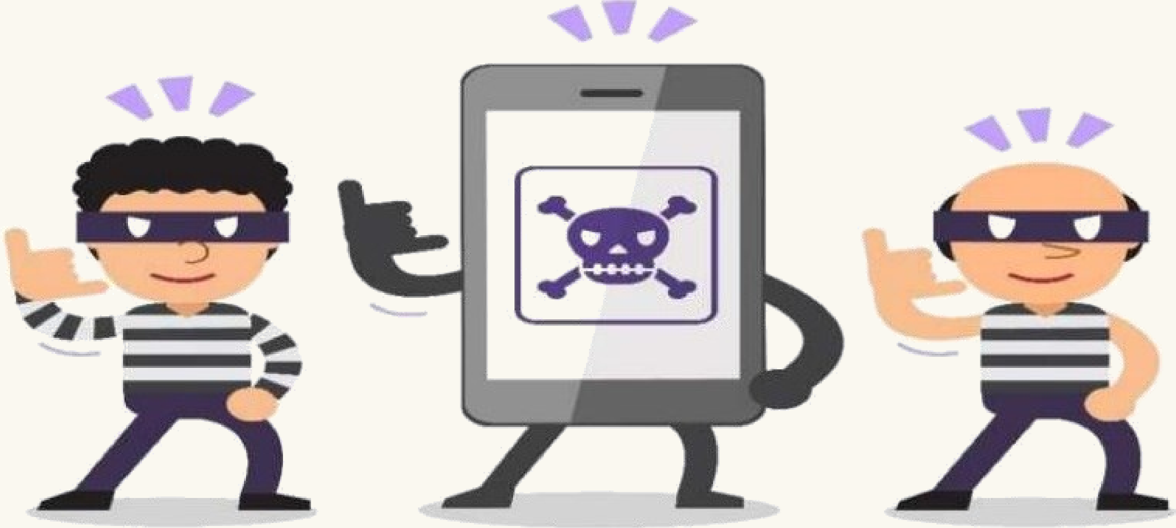
మొబైల్ యాప్‌లో గాని ఆన్ లైన్ లో జరిపే ఆర్థిక లావాదేవీల్లో **ఎల్లప్పుడూ గుర్తుంచుకోండి** : మనం డబ్బులు రిసీవ్ చేసుకొనేటప్పుడు, మనం యెలాంటి 'పాస్ వర్డ్' (Pass word) కాని 'పిన్' (PIN) గాని యివ్వక్కరలేదు. ఒకవేళ అలాంటి ట్రాన్సాక్షన్‌లలో పిన్ టైప్ చేయమని మిమ్మల్ని అడిగితే, మీరు టైప్ చేస్తే , మీ ఎకౌంట్లో వున్న డబ్బులు పోయినట్లే.



4. మనకి తెలియని లేదా అనుమానాస్పద మొబైల్ యాప్స్ ద్వారా జరిగే మోసాలు

నేరాలు చేసే విధానం

- ఒకవేళ మీరు మోసపూరితమైన మొబైల్ యాప్స్‌ని డౌన్‌లోడ్ చేసుకొంటే, మీ మొబైల్ ఫోన్, మీ లాప్‌టాప్, మీ డెస్క్ టాప్ లు మోసగాళ్ళ చేతిలోకి వెళ్తాయి.
- సాధారణంగా యీ లింకులు SMS ద్వారానో, సామాజిక మాధ్యమాల (వాట్సాప్, ఫేస్‌బుక్, ఇంటెర్నెట్, వగైరాల) ద్వారానో, మెస్సెంజెర్‌ల ద్వారానో మీకు పంపబడతాయి. ఇలాంటి లింకులు నమ్మదగినవిగా, ప్రామాణికమైనవిగా కనిపిస్తాయి. నిజానికి కావు. మనల్ని అలాటి నకిలీ యాప్స్‌ని డౌన్‌లోడ్ చేసుకొనేట్లు చేస్తాయి.
- ఒకసారి అలాంటి యాప్ ని డౌన్‌లోడ్ చేసుకొన్నామా – నేరగాళ్ళ చేతుల్లో చిక్కినట్లే.



మనం తీసుకోవలసిన జాగ్రత్త

మీకు తెలియని మొబైల్ యాప్ లను డౌన్‌లోడ్ చేసుకోవద్దు.

5. ఎ.టి.ఎమ్. (ATM) కార్డ్ ల వివరాలు స్కిమ్మింగ్[$] ద్వారా దొంగిలించడం

నేరాలు చేసే విధానం

◊ నేరగాళ్ళు ఎ.టి.ఎమ్ (ATM) వివరాలను స్కిమ్మింగ్ ద్వారా దొంగిలించే పరికరాలని ఎ.టి.ఎమ్ (ATM) మెషీన్లలో ముందుగానే అమర్చి మన కార్డ్లలోని సమాచారాన్ని దొంగిలిస్తారు.

◊ ఒక్కో సారి, ముందే అమర్చబడ్డ అతి సూక్ష్మమైన కెమేరాలద్వారా గాని, డమ్మీ కీ ప్యాడ్ల ద్వారా గాని నేరస్థులు మన పిన్ (PIN) వివరాలను తెలుసుకొంటారు.

◊ డబ్బులు డ్రా చేసుకోవటానికి వచ్చిన కస్టమర్లలాగా నటిస్తూ, మన వెనకాల నిలబడి మన పిన్ గురించిన వివరాలు తెలుసుకొంటారు.

◊ ఆ తరువాత ఒక నకిలీ కార్డ్ ని సృష్టించి, ఆ కార్డ్ ద్వారా మన ఎకౌంట్లలోని డబ్బుని కాజేస్తారు.





మనం తీసుకోవలసిన జాగ్రత్తలు

* ఎ.టి.ఎమ్ (ATM) మెషీన్లో గాని, కీ పాడ్ దగ్గరగాని, ఎ.టి.ఎమ్ రూమ్లో గాని యెలాంటి అనుమానాస్పద పరికరాలు అమర్చలేదని నిర్ధారించుకోండి.
* మీరు మీ పిన్ నంబరు టైప్ చేసేటపుడు చేతిని అడ్డుపెట్టుకోండి.
* మీ వెనకాలో మీ పరిసరాల్లో యెవరైనా మిమ్మల్ని గమనిస్తూ వుంటే మీ పిన్ నంబరు ఎంటరు చేయకండి.
* ఎవ్వరికీ మీ కార్డ్ని యివ్వకండి. మీ పిన్ నంబరు చెప్పకండి.

[$] 'స్కిమ్మింగ్' (Skimming) అంటే ఎ.టి.ఎమ్ (ATM) మెషీన్లలో ఒక పరికరాన్ని అమర్చి డెబిట్ కార్డ్ యొక్క వివరాలన్నీ దొంగిలించడం.



6. స్క్రీన్ షేరింగ్ (Screen sharing) / రిమోట్ షేరింగ్ (Remote sharing) యాప్‌ల ద్వారా నేరాలు చేయడం

నేరాలు చేసే విధానం

- నేరగాళ్ళు మనల్ని నమ్మించి, మన ల్యాప్ టాప్, డెస్క్ టాప్ ల స్క్రీన్ షేర్ చేసుకొనే యాప్‌లను మనచేత మోసపూరితంగా డౌన్ లోడ్ చేయిస్తారు. అలా మనం డౌన్ లోడ్ చేసుకొన్న తరువాత, మన బ్యాంక్ వివరాలన్నీ అంటే బ్యాంక్ ఎకౌంట్ నంబర్, యూజర్ ఐ.డి., పాస్‌వర్డ్, పిన్ (Pin) వగైరాలు తెలుసుకొంటారు.
- తరువాత మన ఇంటర్‌నెట్, మొబైల్ యాప్‌ల ద్వారా మన డబ్బులని డ్రా చేసి వాడుకొంటారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

మీ ల్యాప్ టాప్, డెస్క్ టాప్ స్క్రీన్లని తెలియని వ్యక్తులతో షేర్ చేసుకోవద్దు. లేదా అలాంటి యాప్‌లను డౌన్ లోడ్ చేసుకోవద్దు.



7. ఫోన్ సిమ్ కార్డ్ వివరాలను అపహరించడం

నేరాలు చేసే విధానం

- సాధారణంగా మన బ్యాంక్ ఎకౌంటుకి సంబంధించిన వివరాలన్నీ మన మొబైల్ నంబర్‌కి సంధానం అయి వుంటాయి. నేరగాళ్ళు మన మొబైల్‌లోని సిమ్ కార్డ్ కి అడ్డదోవన కనెక్ట్ అవటమో లేక మన సిమ్ కార్డ్ కి డూప్లికేట్ కార్డ్ ను రూపొందించి దాని ద్వారా ఆన్‌లైన్ లావాదేవీలకు కావలసిన వన్ టైమ్ పాస్ వర్డ్ (OTP) ని తెలుసుకొనో మోసాలకి పాల్పడతారు.
- ఇలా చేయటానికి, నేరస్థులు తాము మొబైల్ / టెలిఫోన్ నెట్‌వర్క్ సిబ్బందిలా నటిస్తూ మనకి ఫోన్ చేసి "మీ సిమ్ కార్డ్ 3జి నుంచి 4జి కి పెంచుతాము" అనో లేకపోతే "మీ సిమ్ కార్డ్ కి అదనపు సౌకర్యాలు కల్పిస్తాము" అనో నమ్మించి మన సిమ్ కార్డ్ వివరాల్ని అపహరిస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

* సిమ్ కార్డ్ గురించిన వివరాలను యెట్టి పరిస్థితుల్లో యెవరికీ చెప్పకండి / షేర్ చేయకండి.
* ఒకవేళ మీ మొబైల్ నెట్‌వర్క్ సాధారణ పర్థితులకు భిన్నంగా చాలా సేపు పని చేయకపోతే మీ సిమ్ కార్డ్ కి డూప్లికేట్ కై ఎవరో ప్రయత్నిస్తున్నారని మీకు అనుమానం రావాలి. వెంటనే మొబైల్ ఆపరేటర్‌కి ఫోన్ చేసి యెలాంటి డూప్లికేట్ సిమ్ కార్డ్ జారీ చేయొద్దని ఆదేశాలు యివ్వండి.



8. ఇంటర్‌నెట్ లోని సెర్చ్ ఇంజెన్స్ ద్వారా మన వివరాలను దొంగిలిచండం

నేరాలు చేసే విధానం

- సహజంగా మనం చాలాసార్లు నెట్ బ్యాంకింగ్‌కి అయినా, ఇన్సురెన్స్, ఆధార్‌కి సంబంధించిన అంశాలకైనా, సెర్చ్ ఇంజన్స్‌ని బ్రౌజ్ చేస్తాం. (ఉదా: గూగుల్, బింగ్, మైక్రోసాఫ్ట్, యాహూ వగైరాలు). ఒక్కోసారి మనకి తెలియకుండానే మనం అధికారిక (Official) వెబ్‌సైట్లని వదిలేసి నకిలీ (Duplicate) వెబ్‌సైట్లలోకి వెళ్ళటం జరుగుతుంది. అలాంటప్పుడు నేరగాళ్ళ చేతిల్లోకి మనకి తెలియకుండానే మనం వెళ్ళిపోయినట్లే.
- ఒకసారి ఆ సైట్లలోకి వెళ్తే, నేరగాళ్ళు మన బ్యాంక్ వివరాలు, యూజర్ ఐ.డి., సి.వి.వి లాంటి కీలక సమాచారాన్ని / వివరాల్ని "పరిశీలించాలి" అని నమ్మించి మన దగ్గర నుంచి రాబడతారు. అలా ఆ దొంగ వెబ్‌సైట్ల ద్వారా మన వివరాలని సేకరించి ఆర్థిక నేరాలకు పాల్పడతారు.
- అలాంటి వెబ్‌సైట్లని నిజమైనవిగా నమ్మి, చాలా మంది మోసపోతారు – కష్టపడి సంపాదించుకొన్న సొమ్ముని పోగొట్టుకొంటారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

కస్టమర్ కేర్ వివరాలకై సెర్చ్ ఇంజన్స్‌లోకి వెళ్ళకండి. చాలా సార్లు నేరగాళ్ళు వీటిని అక్రమంగా అందబుచ్చుకొంటారు. ఎల్లప్పుడు అధికారిక (official) వెబ్ సైట్‌లనే (బ్యాంకులుగాని, ఇన్సూరెన్స్ కంపెనీలుగాని, ఆధార్ గానీ) బ్రౌజ్ చేయండి. మీకు కావలసిన వివరాలను పొందండి.



9. క్యూ.ఆర్. (QR)[$] స్కానింగ్ ద్వారా మోసపూరితంగా డబ్బులు దోచేయడం

నేరం చేసే విధానం

- ఏదో సాకు చెప్పి, కస్టమర్లని ప్రలోభ పరిచి పేమెంట్ యాప్స్ ద్వారా క్యూ.ఆర్. (QR) కోడ్స్‌ని స్కాన్ చేయించి కస్టమర్ల ఎకౌంట్ లోని డబ్బుల్ని కాజేస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

క్యూ.ఆర్. (QR) కోడ్లని స్కాన్ చేసేటప్పుడు తగు జాగ్రత్త వహించాలి.
క్యూ.ఆర్. (QR) కోడ్లలో మన ఎకౌంట్ల వివరాలన్నీ నిక్షిప్తమై వుంటాయి.
ఆ వివరాలతో మన ఎకౌంట్లలోని డబ్బుల్ని కాజేస్తారు.

$ QR code (Quick Response Code) : A QR code is a type of matrix barcode invented in 1994 by the Japanese automotive company Denso Wave. A barcode is a machine-readable optical label that contains information about the item to which it is attached.



10. సామాజిక మాధ్యమాలలో మన పేర్ల మీద ఎకౌంట్లు సృష్టించి మోసాలకి పాల్పడటం. (Impersonfication)

నేరాలు చేసే విధానం

- నేరగాళ్ళు ఫేస్ బుక్, ఇన్స్టాగ్రామ్, మొదలైన సామాజిక మాధ్యమాల్లో మన పేరు మీద ఎకౌంట్లు సృష్టిస్తారు. మందులు కొనటానికి డబ్బులు కావాలనో, అత్యవసరమయ్యిందనో మనం అడుగుతున్నట్లుగా భ్రమ కల్పించి మన స్నేహితులనుండి, బంధువులనుండి డబ్బులు వసూలు చేస్తారు.
- అలా నమ్మించి, మన పేరు వాడుకొంటూ మన స్నేహితులని, మన బంధువులని బ్లాక్ మెయిల్ చేసో, బెదిరించో, ఘరానాగా డబ్బులు దోపిడీ చేస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

* గుర్తు తెలియని కొత్తవారికి ఆన్‌లైన్‌లో డబ్బులు పంపకండి.
* వ్యక్తిగత ఆర్థిక వివరాలను (ఎకౌంట్ నంబరు, యూజర్ ఐ.డి., పాస్ వర్డ్, ఒ.టి.పి వగైరాలు) సామాజిక మాధ్యమాలలో యెట్టి పరిస్థితుల్లో పోస్ట్ చేయకండి.
* ఒకవేళ మీకలాంటి మెసేజ్ మీ స్నేహితులనుంచో బంధువులనుంచో వస్తే , వారికి ఫోన్ ద్వారానో లేదా వారిని కలుసుకొనో అది మోసపూరితమైన మెసేజ్ కాదని నిర్ధారించుకొన్న తరువాతే డబ్బులు పంపండి. తొందర పడకండి.



11. మనం మొబైల్ చార్జ్ చేసుకొనే పోర్ట్ ద్వారా మన వివరాలను కాజేయడం (Juice jacking)

నేరాలు చేసే విధానం

◊ మనం బయట వుపయోగించుకొనే మొబైల్ చార్జింగ్ పోర్ట్ నుంచి కూడా మన ఫోన్‌లోని డాటానిగాని యితర ఆర్థిక వివరాలను గాని దొంగిలించే అవకాశం వుంది. దీన్నే "జ్యూస్ జాకింగ్" (Juice jacking) అని అంటారు.

◊ "జ్యూస్ జాకింగ్" ద్వారా మన మొబైల్ ఫోన్లలోకి ప్రమాదకరమైన 'మాల్‌వేర్' ను పంపించి దాని ద్వారా మన మెసేజీలను, ఇ-మెయిల్స్‌ను, మనం భద్రపరచుకొన్న పాస్‌వర్డ్స్‌ను, యితర వివరాలను కంట్రోల్ చేయవచ్చు లేదా కాజేయవచ్చు.



మనం తీసుకోవలసిన జాగ్రత్త

* బహిరంగ ప్రదేశాల్లోని లేదా మనకి తెలియని ప్రదేశాల్లోని పోర్ట్‌లద్వారా మన మొబైల్ ఫోన్లను చార్జి చేసుకోవద్దు.



12. లాటరీ పేరుతో జరిగే మోసాలు (Lottery fraud)

నేరాలు చేసే విధానం

- ◊ నేరగాళ్ళు ఫోన్ ద్వారానో, ఇ-మెయిల్ ద్వారానో మీకు పెద్ద మొత్తంలో లాటరీ వచ్చిందని ఓ సందేశం పంపుతారు. అలా మీకొచ్చిన డబ్బుని పంపిచాలంటే "మీ బ్యాంక్ ఎకౌంట్, యితర వివరాలు పరిశీలించాలి" అని మాయమాటలు చెప్పి, మీ వివరాలన్ని మీ నుంచి రాబడతారు.
- ◊ కొన్ని కేసుల్లో, లాటరీ డబ్బులు పంపాలంటే ముందుగానే టాక్సులు చెల్లించాలనో, పోస్టేజి / షిప్పింగ్ చార్జీలు భరించాలనో, ప్రాసెసింగ్ చార్జీలు చెల్లించాలనో యెంతో కొంత డబ్బు పంపమని నేరగాళ్ళు వత్తిడి తెస్తారు.
- ◊ వాళ్ళు చెల్లించమనే డబ్బు మీకొచ్చిందన్న లాటరీ డబ్బుతో పోల్చుకొంటే చాలా తక్కువవవటంతో వాళ్ళ మాటలు నమ్మిన చాలా మంది మోసపోయి డబ్బు పంపిస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

- * అలాంటి మొబైల్ కాల్స్‌కి, ఇ-మైల్స్ కి యెట్టి పరిస్థితుల్లో స్పందించకండి.
- * మీరు యే టికెట్ కొనకుండానే మీకంత పెద్ద మొత్తంలో లాటరీ వచ్చిందంటే మీరు యెలా నమ్ముతారు ? నిస్సందేహంగా అది మోసమే.



13. ఉద్యోగాలిస్తామని ఆన్ లైన్‌లో జరిగే మోసాలు (Online job fraud)

నేరాలు చేసే విధానం

- నేరస్థులు ముందుగా నకిలీ (దొంగ) జాబ్ పోర్టల్స్ ని సృష్టిస్తారు. ఉద్యోగం వస్తుందనే ఆశతో కొందరు అమాయకులు ఆ పోర్టల్‌ని బ్రౌజ్ చేస్తే, రిజిస్ట్రేషన్ సాకుతో అభ్యర్థి బ్యాంక్ ఎకౌంట్లు, తదితర కీలక వివరాలను కాజేస్తారు.
- కొన్నిసార్లు నేరస్థులు పేరొందిన కంపెనీల అధికారులుగా తమకు తామే పరిచయం చేసుకొని, దొంగ ఇంటర్వ్యూలు నిర్వహించి, సెలెక్ట్ అయినట్లు అభ్యర్థులకు తెలియజేస్తారు. ఆపైన ట్రైనింగనో, కాషన్ డిపాజిట్టనో యేదో సాకుతో డబ్బులు వసూలు జేస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

ఏ కంపెనీ ఉద్యోగమిచ్చేటప్పుడు డబ్బులు అడగదు.

ఎట్టి పరిస్థితుల్లో ఆన్‌లైన్ జాబ్ పోర్టల్స్‌లో డబ్బులు పంపకండి.







పార్ట్ - బి
(Part - B)

నాన్ బ్యాంకింగ్ ఫైనాన్షియల్ కంపెనీలు
(Non-Banking Financial Companies)





1. లోన్లు యిస్తామని దొంగ ప్రకటనలు

నేరాలు చేసే విధానం

- ◊ "అతి తక్కువ వడ్డీ రేటుతో, ఏ మాత్రం సెక్యూరిటీలు, గ్యారంటీలు లేకుండా, ప్రాసెసింగ్ ఫీజులు లేకుండా, సులభ వాయిదా పద్ధతుల్లో లోన్లు యిస్తాం. మమ్మల్ని సంప్రదించండి" అని నేరస్థులు కల్లబొల్లి ప్రకటనలు చేస్తారు.
- ◊ ఇలాంటి అబద్ధపు ప్రకటనలు నిజమైనవిగా నమ్మించటానికి పేరున్న బ్యాంకింగేతర ఆర్థిక సంస్థల (NBFCs) అధికార్ల పేర్లు, వారి ఇ-మెయిల్స్ వాడుకొంటారు.
- ◊ వీళ్ళ మాటలు నమ్మి, యెవరైనా వీరిని సంప్రదిస్తే, వెంటనే, మీ లోన్ మంజూరు అయిందని, లోన్ డబ్బులు పంపించాలంటే, ప్రాసెసింగ్ ఫీజ్ కి అని, జి.ఎస్.టి. (GST) కి అని అడ్వాన్స్ ఇ.ఎమ్.ఐ. (EMI) ఇన్స్టాల్మెంట్ కి అని, ఇంటర్ సిటీ చార్జిలనీ, యేవేవో పేర్లు చెప్పి, కొంత డబ్బు పంపమంటారు. ఒకవేళ అమాయకంగా డబ్బు పంపితే మాయమైపోతారు. వాళ్ళ ఆచూకీయే వుండదు.
- ◊ నేరస్థులు వాళ్ళ వాళ్ళ వెబ్సైట్లను కూడా సృష్టించుకొని, అప్పు కావలనుకోనే వాళ్ళకోసం వల పన్నుతూ వుంటారు



మనం తీసుకోవలసిన జాగ్రత్తలు

- ⁎ ఎన్.బి.ఎఫ్.సి.లు గాని బ్యాంకులుగాని లోన్ అప్లికేషన్లు ప్రాసెసింగ్ ఫీ లాంటివి వసూలు చేయరు.
- ⁎ బ్యాంకులు అలాంటి ప్రాసెసింగ్ ఫీజులను లోన్ మంజూరయింతర్వాత, లోన్ మొత్తం యిచ్చేటప్పుడు వసూలు చేస్తారు. ముందుగా వసూలు చేయరు.
- ⁎ ఎట్టి పరిస్థితుల్లోనూ, మీ బ్యాంక్ తదితర వివరాలను అలాంటి వారికి తెలియజేయకండి. అలాంటి సైట్లలోకి వెళ్ళే ముందు వాటి నిబద్ధతను మరీ పరిశీలించండి.



2. SMS / ఇ-మెయిల్ / మెస్సేజింగ్ / ఫోన్ల ద్వారా జరిగే మోసాలు

నేరాలు చేసే విధానం

- SMS ల ద్వారాగాని, యితర సామాజిక మాధ్యమాల ద్వారా గాని, పేరొందిన బ్యాంకింగేతర సంస్థల (NBFCs) లోగో లని ఫోన్లలో ప్రొఫైల్ పిక్చర్ల లా వాడుకుంటూ తక్కువ వడ్డీతో, యే సెక్యూరిటీలు లేకుండా సులభ పద్ధతుల్లో అప్పులు యిస్తామని మెసేజీలు పంపుతూ ఆకర్షిస్తారు.
- అలా సాముహికంగా మెసేజీలు పంపిన తరువాత, నేరస్థులు కొంతమందిని యెంచుకొని వాళ్ళకి లోన్ మంజూరు చేసినట్లు పత్రాలను, మంజూరు అయిన మొత్తానికి నకిలీ చెక్కులను పంపుతూ, ప్రాసెసింగ్ చార్జీలకనో యితర ఖర్చులకనో కొంత డబ్బు వసూలు చేస్తారు. ఒకసారి డబ్బులు అందిన తరువాత యీ నేరస్థుల ఆచూకే వుండదు.



మనం తీసుకోవలసిన జాగ్రత్తలు

- మనకు తెలియని వ్యక్తుల వద్దనుంచి వచ్చిన అలాంటి మెసేజిలను పట్టించుకోకండి. వాటికి స్పందించి, ఆ మోసగాళ్ళతో యెలాంటి సంప్రదింపులు జరపకండి.
- మనం అడక్కుండానే, వాళ్ళకై వాళ్ళు మనకి ఫోన్ చేసి "అప్పు యిస్తాం" అంటే మనం యెలా నమ్మాలి ? ఎందుకు నమ్మాలి ?
- గుర్తు తెలియని వ్యక్తులకు వాళ్ళ వివరాలు తెలియకుండా యెట్టి పరిస్థితుల్లోనూ డబ్బు పంపకండి.



3. ఓ.టి.పి (OTP) దొంగిలించి చేసే మోసాలు

నేరాలు చేసే విధానం

- నేరస్థులు తాము పేరొందిన NBFCs నుంచి మాట్లాడుతున్నామని, పెద్ద మొత్తాల్లో లోన్లు యిస్తామని లేదా క్రెడిట్ లిమిట్ పెంచుతామని, మాయ మాటలు చెపుతూ, SMS / ఇన్స్టంట్ మెసేజీలో పంపి, వాళ్ళ మొబైల్ నంబర్లకి ఫోన్ చేసి మాట్లాడమంటారు.
- అమాయకంగా వాళ్ళ మాటలని నమ్మి, వారితో మాట్లాడితే, ఆన్‌లైన్ ద్వారా లోన్ అప్లికేషన్ పంపమంటారు. ఆ అప్లికేషన్‌లో మన బ్యాంక్ ఎకౌంట్‌కి సంబంధించిన అన్ని వివరాలూ వుంటాయి. ముఖ్యంగా, ఆ అప్లికేషన్‌ని ప్రాసెస్ చేస్తున్నట్లు నటిస్తూ, మన ఎక్కౌంట్లో నుంచి డబ్బులు డ్రా చేయటానికి కావలసిన వివరాలన్నింటిని అంటే పిన్ (PIN), ఓ.టి.పి. (OTP), లను మననుంచి రాబట్టి, డబ్బులు కాజేస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

* మీ యూజర్ ఐ.డి. గాని, మీ పాస్‌వర్డ్ గాని, మీ కార్డ్ వివరాలుగాని, CVV (Card verification value) గాని, వన్ టైమ్ పాస్ వర్డ్ (OTP) గాని యెట్టి పరిస్థితుల్లోను యెవరికీ యివ్వకండి.
* తరచుగా మీ SMS, మీ ఈ-మైల్స్ చూసుకోండి. మీ బ్యాంక్ ఓ.టి.పి. యెవరైనా మీకు తెలియకుండా మారిస్తే తెలుస్తుంది.



4. మోసపూరిత వెబ్‌సైట్లు / యాప్‌లలో జరిగే మోసాలు

నేరాలు చేసే విధానం

- లోన్లు అప్పటికప్పుడు ఇస్తామంటూ ప్రలోభ పెట్టే మోసపూరిత వెబ్‌సైట్‌లు ఈ మధ్య చాలా పుట్టుకొచ్చాయి. ఇవి ప్రజలను మోసం చేస్తూ అత్యధిక వడ్డీలను వసూలు చేస్తున్న సంఘటనలు చాలా వెలుగులోకి వచ్చాయి.
- అమాయక ప్రజలని ఆకర్షించి, వారిని తమ వలలో వేసుకోవటానికి, "ఈ ఆఫర్ చాలా కొద్ది రోజులు మాత్రమే", "త్వరగా నిర్ణయం తీసుకోండి" అంటూ స్కేర్ వేర్$ (Scareware) టెక్నిక్స్ ద్వారా మభ్యపెడుతూ వుంటారు.
- అలాంటి మోసపూరిత వెబ్‌సైట్లలో లోన్లు తీసుకొనేముందు ఈ క్రింది విషయాలను



- "అప్పిచ్చేవాడు అప్పుకి సంబంధించిన విషయాలని పరీక్షిస్తున్నాడా లేకపోతే మన వ్యక్తిగత బ్యాంకింగ్ వివరాల మీద యెక్కువ శ్రద్ధ చూపిస్తున్నాడా ? ", "అప్పు ఇచ్చే సంస్థ ప్రభుత్వంతోనో లేక యే ఇతర ఏజెన్సీతో రిజిస్టర్ అయి వుందా లేదా ?", "అలా అప్పిచ్చే వాడు తన అడ్రెస్, ఫోన్ నంబర్లు, తదితర విషయాలు మీకు అందజేసాడా లేదా ?" ఇలాంటి అనుమానాలను నివృత్తి చేసుకోండి. లేకపోతే తరువాత వారిని సంప్రదించాలంటే కష్టమవుతుంది.
- మీరు బ్రౌజ్ చేసే సైట్లు అసలైనవో కావో ఒకటి రెండు సార్లు పరీక్షించండి.

గుర్తుంచుకోండి

- ఏ బ్యాంకు గాని బ్యాంకింగేతర సంస్థ (NBFC) గాని లోన్ మంజూరు చేసేముందు, మిమ్మల్ని డబ్బు కట్టమని అడగదు.
- నిజంగా అప్పు ఇచ్చేవాడు మన ఆస్తి వివరాలు, తదితర డాక్యుమెంట్లు పరిశీలించకుండా లోన్లు మంజూరు చేయరు.

$ Malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection.



5. మనీ సర్క్యులేషన్, పొంజీ డిపాజిట్లు (వేరే వ్యాపకం గాని వ్యాపారం లేకుండా డిపాజిట్లను సేకరించి, వాటిని చెల్లించటానికి కొత్త డిపాజిట్లను వాడుకోవటం), కొన్ని మార్కెటింగ్ స్కీముల ద్వారా జరిగే మోసాలు

- ◊ పైన చెప్పబడ్డ స్కీముల్లో మనం డిపాజిట్లు చేసినా, చేయించినా, వెంటనే కొన్ని నగదు బహుమానాలు యిస్తామని వాగ్దానాలు చేస్తారు.
- ◊ అలా డిపాజిట్ చేయబడ్డ వాటి పైన అత్యధిక వడ్డీలను యెరగా చూపుతారు. నమ్మకం కలిగించటానికి, ముందు కొన్ని డిపాజిట్లను అనుకొన్న గడువునాటికి చెల్లిస్తారు. అలా తాము నిజాయితీపరులమని, తమది నికార్సైన కంపెనీ అని ప్రచారం చేయించుకొంటారు.
- ◊ మనీ సర్క్యులేషన్ లో మరింతమంది సభ్యులను చేర్పించుకొని, కమీషన్‌లు యిస్తూ పోతూ వుంటారు. నిజానికి అక్కడ యే వ్యాపారమూ జరగదు. ఏ వస్తువులూ వుత్పత్తి గావు. కొన్ని రోజులకి ఆ స్కీముల్లో చేరే సభ్యుల సంఖ్య నెమ్మదిగా తగ్గిపోతుంది. అలా కొన్ని రోజుల తరువాత, అలాంటి స్కీములు నెమ్మదిగా కనుమరుగవుతాయి. ఆ తరువాత, వసూలు చేసుకొన్న సొమ్ముతో నేరస్థులు వుడాయిస్తారు.



మనం తీసుకోవలసిన జాగ్రత్తలు

- మన పెట్టుబళ్ళ మీద వచ్చే ఆదాయం – అలాంటి పెట్టుబడులలో వుండే రిస్క్ మీద ఆధార పడి వుంటుంది. ఎక్కువ ఆదాయం వస్తుందంటే ఎక్కువ రిస్క్ వున్నట్లే. ఏ స్కీం అయినా మనం వూహించని విధంగా అత్యధిక వడ్డీ (ఉదాహరణకి సాలుకి 40 నుంచి 50 శాతం వరకు) యిస్తామని ఆఫర్ చేస్తే – అలాంటి స్కీములు ఖచ్చితంగా మోసపూరితమైనవని అర్థం చేసుకోవాలి. నేరస్థులు చేయబోయే మోసానికి యిది ప్రథమ ఘంటిక.
- ఏ వ్యాపారం లేకుండా / ఎలాంటి వస్తువుల్ని వుత్పత్తి చేయకుండా, "కమీషన్లు/బోనస్లు యిస్తాము, లాభాల్లో వాటా యిస్తాము" అంటూ కపట వాగ్దానాలు చేశారో – అలాంటి కంపెనీలు నూటికి నూరు పాళ్ళు మోసపురితమైనవని, నిలువునా ముంచేవని అర్థం చేసుకోవాలి.
- మనీ సర్క్యులేషన్ చైన్ స్కీముల్ని, పిరమిడ్ డిపాజిట్ స్కీముల్ని, దొంగ మార్కెటింగ్ స్కీముల్ని యెట్టి పరిస్థితుల్లో నమ్మకండి.
- పైన చెప్పబడ్డ యే స్కీమ్ ద్వారా అయినా ప్రజలనుంచి డబ్బులు స్వీకరించడం "ప్రైజ్ చిట్ & మనీ సర్క్యులేషన్ (బానింగ్) యాక్ట్, 1978" క్రింద నేరమూ, శిక్షార్హం. అలాంటి స్కీములతో యెవరైన మీకు తారసపడితే వెంటనే, పోలీస్ రిపోర్ట్ యివ్వండి.



6. నకిలీ పత్రాలు సృష్టించి అప్పు తీసుకొని పారిపోవటం

- ఒక వ్యక్తి గాని, సంస్థ గాని నకిలీ పత్రాలు సృష్టించి వాటిని తాకట్టు పెట్టి ఆర్థిక సంస్థలనుంచి లోన్లు, మరియు యితర సేవలను పొందటం యీ రకమైన ఆర్థిక నేరాలుగా పరిగణింపబడతాయి.
- కె.వై.సి. (KYC) పత్రాల్ని మనకేమాత్రం పరిచయం లేని వారికి యివ్వటం లేదా ఇ-మెయిల్‌లో గుర్తు తెలియని వ్యక్తులకి, లేదా నకిలీ ఎన్.బి.ఎఫ్.సి (NBFC) ఇ-మెయిల్స్ కి పంపటం ద్వారా యిలాంటి మోసాలు జరిగే అవకాశం వుంటుంది.
- ఒక్కోసారి, నేరస్థులు మన వ్యక్తిగత వివరాలని, అంటే ఐడింటిటీ కార్డులు, బ్యాంక్ ఎకౌంట్లు లాంటివి మన దగ్గరనుంచి దొంగిలించి యేదైనా బ్యాంకునుండి గాని మరే యితర ఎన్.బి.ఎఫ్.సి (NBFC) ల నుంచి గాని మన పేర ఋణాలు తీసుకొని మోసం చేసే అవకాశం వుంది.



మనం తీసుకోవలసిన జాగ్రత్తలు

* ఏ ఆర్థిక సంస్థనుంచి అయినా (బ్యాంక్ గానీ ఎన్.ఎఫ్.బి.సి గాని) అప్పు తీసుకొంటున్నప్పుడు, మీకు సంబంధించిన కె.వై.సి. (KYC) వివరాలనుగాని, మీ ఆస్తులకి సంబంధించిన డాక్యుమెంట్లను గాని, మీ బ్యాంకు ఎకౌంట్ వివరాలనుగాని యిచ్చేటప్పుడు తగిన జాగ్రత్త వహించండి.
* ఆ సంస్థ యొక్క అధికారులకి మాత్రమే అందజేయండి. ఆన్‌లైన్‌లో పంపుతుంటే ఆ సంస్థల అధికృత (official) వెబ్‌సైట్‌లోనే పంపండి.
* ఒకవేళ, యే కారణం చేతనైనా, లోన్ మంజూరు కాకపోతే, మీరు వారికిచ్చిన డాక్యుమెంట్లను తిరిగి తీసుకోవటం యెట్టి పరిస్థితుల్లోనూ మరచిపోవద్దు.



ఆన్‌లైన్ ట్రాన్సాక్షన్లలో
మనం తీసుకోవలసిన మరిన్ని జాగ్రత్తలు

PART-C



ప్రాధమికంగా తీసుకోవలసిన జాగ్రత్తలు

- మీకు అనుమానం వున్న వెబ్ సైట్లు, టెలెఫోన్లలో వచ్చే మెసేజీలు, "పాప్ అప్స్ ల జోలికి వెళ్ళకండి.
- పేమెంట్ గేట్‌వే లో ఆన్‌లైన్ పేమెంట్ చేస్తున్నప్పుడు, యీ క్రింద చూపించినట్లుగా, "తాళం" గుర్తు వున్నదా లేదా చూసుకొండి. ఉంటేనే లావాదేవీలు జరపండి.



- మీ కార్డ్ డిటైల్స్, యూజర్ ఐ.డిలు, పాస్ వర్డ్, సి.వి.వి. నంబర్లు, క్రెడిట్ / డెబిట్ కార్డ నంబర్లు మొదలైనవి మీ దగ్గరే జాగ్రత్తగా వుంచుకోండి.
- ఆ వివరాలను మీ లాప్ టాప్‌లలో గాని, యితర వెబ్‌సైట్లలో గాని సేవ్ చేయకండి.
- ఆన్‌లైన్ ట్రాన్సాక్షన్లలో రెండు పాస్ వర్డ్‌లు వాడే విధానం ఒక వేళ వుంటే దానిని వుపయోగించుకోండి.
- మీకు తెలియని వాళ్ళ దగ్గరనుంచి వచ్చిన ఇ-మెయిల్స్‌ని గాని, వాటి ఎటాచ్‌మెంట్లనుగాని, ఫిషింగ్ లింక్స్‌ని గాని యెట్టి పరిస్థితుల్లో చూడకండి/ తెరవకండి.
- మీ బ్యాంక్ చెక్ కాపీని గాని, మీ కె.వై.సి. డాక్యుమెంట్ల కాపీలనుగాని అవసరమైన వాళ్ళతో మాత్రమే షేర్ చేయండి.



మొబైల్ డివైస్‌లు / కంప్యూటర్ సెక్యూరిటీకై తీసుకోవలసిన జాగ్రత్తలు

- మీ పాస్ వర్డ్ ని తరచుగా మార్చుకొంటూ వుండండి.
- మీ కంప్యూటర్లలో "యాంటీ వైరస్" ని యిన్‌స్టాల్ చేసుకొని యెప్పటికప్పుడు అప్‌డేట్ చేసుకోంటూ వుండండి.
- కంప్యూటర్లను వాడని సమయాల్లో లాక్ చేసి వుంచండి. ఆటో లాక్ సదుపాయాన్ని వాడుకోండి.
- మనకి తెలియని లేదా అనుమానస్పద యాప్స్ ని లేదా సాఫ్ట్ వేర్‌ని లోడ్ చేసుకోకండి.
- మీ పాస్‌వర్డ్‌ని యితర సిస్టంలలో సేవ్ చేయకండి.





సురక్షిత "ఇంటర్నెట్ బ్యాంకింగ్" కోసం విధిగా మనం చేయవలసినవి.

* ఏ వెబ్‌సైట్ పడితే ఆ వెబ్‌సైట్ జోలికి వెళ్ళకండి.
* మనకి తెలియని బ్రౌజర్లను వాడకండి.
* పాస్‌వర్డ్‌ని బయట కంప్యూటర్లలో సేవ్ చేయకండి.
* సామాజిక మాధ్యమాలలో (వాట్సాప్, ఫేస్‌బుక్, టెలిగ్రామ్, మొదలైనవి) వ్యక్తిగత విషయాలను సేవ్ చేయకండి.
* మీకొచ్చిన ఈ-మెయిల్ ని గాని, ఎస్.ఎమ్.ఎస్. (SMS) మెసేజిని గాని యితరులకి పంపే ముందు దాని సెక్యూరిటీ పరీక్షించండి.
* ఇంటెర్నెట్ బ్యాంకింగ్‌లో 'వర్చ్యువల్' (virtual) కీ బోర్డ్‌ని, క్రింద ఫొటోలో చూపించిన విధంగా, వుపయోగించండి. ఒక్కో సారి మనం టైప్ చేసినదాన్ని వేరే పరికరాల ద్వారా కాపీ చేసే ప్రమాదం వుంది.
* ఒకసారి నెట్ బ్యాంకింగ్ లో మీ ట్రాన్సాక్షన్ అయిపోయిన వెంటనే, "లాగ్ ఔట్" అవ్వండి.
* మీ పాస్ వర్డ్‌ని యెప్పటికప్పుడు అప్‌డేట్ చేసుకోండి.
* మీ ఇ-మెయిల్‌కి, మీ ఇంటెర్నెట్ బ్యాంకింగ్‌కి ఒకే పాస్‌వర్డ్‌ని వాడకండి.
* సైబర్ కేఫ్ లాంటి వాటిల్లోని కంప్యూటర్లలో వీలైనంతవరకు బ్యాంకింగ్ ట్రాన్సాక్షన్స్‌ని చేయకండి.





ఇ-మెయిల్ ఎకౌంట్ సెక్యూరిటీ కోసం మనం తీసుకోవలసిన జాగ్రత్తలు

* మనకు సంబంధించని లేదా తెలియని వాళ్ళనుంచి వచ్చిన ఇ-మెయిల్స్‌ని క్లిక్ చేయకండి.
* పబ్లిక్ స్థలాల్లోని కంప్యూటర్లలో మీ ఇ-మెయిల్స్‌ని చూడకండి.
* మీ బ్యాంక్ ఎకౌంట్లు, పాస్‌వర్డ్స్ లాంటి ముఖ్య సమాచారాన్ని ఇ-మెయిల్స్‌లో వుంచకండి.



పాస్ వర్డ్స్ సెక్యూరిటీకై తీసుకోవలసిన జాగ్రత్తలు

* మీ పాస్‌వర్డ్స్‌లో ఆల్ఫాన్యుమరిక్ (అంటే అంకెలు, సంఖ్యలు జోడించినవి) మరియు ప్రత్యేక క్యారెక్టర్స్ (అంటే @,#,$,%,& లాంటివి) తప్పనిసరిగా వాడండి.
* ఒకవేళ రెండు చోట్ల రెండు రకాలైన పాస్‌వర్డ్స్ ని వాడుకొనేవిధానం వుంటే ఆ సౌకర్యాన్ని వాడుకోండి.





బ్యాకింగేతర సంస్థలు (NBFCలు) డిపాజిట్లు సేకరించడానికి రిజర్వ్ బ్యాంక్ వారిచే ఆమోదింపబడ్డ సంస్థలో కాదో యెలా తెలుసుకోవాలి ?

* అలా తెలియాలంటే రిజర్వ్ బ్యాంక్ వారి వెబ్ సైట్ rbi.org.in దర్శించి, "ఆ NBFC రిజర్వ్ బ్యాంక్ వారిచే డిపాజిట్లు సేకరించడానికి నిషేధింపబడ్డ సంస్థ కాదు" అని నిర్ధారించుకోండి.
* NBFC లు తమ తమ వెబ్ సైట్లలో రిజర్వ్ బ్యాంక్ వారిచే జారీ చేయబడ్డ "రిజిస్ట్రేషన్ సర్టిఫికేట్" ని వుంచాలి.
* రిజిస్ట్రేషన్ సర్టిఫికేట్లు జారీ చేయబడ్డా, రిజర్వ్ బ్యాంక్ వారు ఆమోదిస్తేనే ఆ సంస్థ ప్రజలనుంచి డిపాజిట్లను స్వీకరించాలి.
* NBFC లు స్వీకరించిన డిపాజిట్ల మీద సాలుకి 12.5 శాతం కంటె యెక్కువ వడ్డీ చెల్లించ రాదు.
* మరియు NBFC లు 12 నెలల లోపు, 60 నెలలకంటే ఎక్కువ కాలానికి డిపాజిట్లను స్వీకరించరాదు.
* ఒకవేళ రిజర్వ్ బ్యాంక్ వారు NBFCలు చెల్లించవలసిన వడ్డీ రేట్లలో మార్పు తీసుకువస్తే యీ క్రింది వెబ్ సైట్‌లో తెలియజేస్తారు.

https://rbi.org.in → Sitemap → NBFC List → FAQs.





డిపాజిటర్లు తీసుకోవలసిన జాగ్రత్తలు

* ఎన్.బి.ఎఫ్.సి. లో ఎప్పుడు డిపాజిట్ చేసినా, అలా జమ చేసిన మొత్తానికి సరి అయిన రసీదు తీసుకొండి.
* అలా యివ్వబడ్డ రసీదుపై ఆ ఎన్.బి.ఎఫ్.సి. (NBFC) యొక్క అధికారిక సీలు, డిపాజిట్ చేసిన తేదీ, డిపాజిట్ చేసిన వ్యక్తి పేరు, డిపాజిట్ మొత్తం (అక్షరాలలోనూ, అంకెలలోనూ), ఆ డిపాజిట్ పై వచ్చే వడ్డీ, డిపాజిట్ కాల వ్యవధి ముగిసే రోజు లాంటి వివరాలు తప్పనిసరిగా వ్రాసి వుండాలి.
* ఇక్కడ డిపాజిటర్లు గమనించవలసినది – ఎన్.బి.ఎఫ్.సి. (NBFC) లలో డిపాజిట్ చేసిన మొత్తాలకు డిపాజిట్ ఇన్సురెన్స్ వర్తించదు.





ఆన్‌లైన్ కంప్లైంట్ యెలా చేయాలి ?

Complaint to RBI (ఆర్.బి.ఐ. కి కంప్లైంట్ చేయాలంటే..)

Please visit the link at https://cms.rbi.org.in/

Complaint to SEBI (సెబి కి కంప్లైంట్ చేయాలంటే..)

Please visit the link at https://scores.gov.in/

Complaint to Insurance Regulatory and Development Authority of India (IRDAI) (ఐ.ఆర్.డి.ఎ.ఐ.) కి కంప్లైంట్ చేయాలంటే

Please visit the link at https://igms.irda.gov.in/

Complaint to National Housing Bank (NHB) (ఎన్.హెచ్.బి. సెబి కి కంప్లైంట్ చేయాలంటే)

Please visit the link at https://grids.nhbonline.org.in/

Complaint to Cyber Police Station (సైబర్ పోలీస్ స్టేషన్ కి కంప్లైంట్ చేయాలంటే)

Please visit https://cybercrime.gov.in/







రిజర్వ్ బ్యాంక్, ముంబై-2 (అంబుడ్స్‌మన్) వారు ముద్రించిన"Be(A)ware" అనే పుస్తకానికి
తెలంగాణ రాష్ట్ర సహకార అపెక్స్ బ్యాంక్, సహకార శిక్షణా సంస్థ (CTI) , హైదరాబాద్ వారి
తెలుగు అనువాదం.